NOT ENTERED

AMENDMENTS TO THE CLAIMS

THIS LISTING OF CLAIMS WILL REPLACE ALL PRIOR VERSIONS, AND LISTINGS OF CLAIMS IN THE APPLICATION.

1. (Currently amended) A method for detecting spurious network traffic comprising:

receiving a packet, the packet including data for transmission over a network;

calculating a plurality of possible ports from which the packet is expected to be received using a source network address of the packet, wherein each one of the plurality of possible ports has associated therewith a weight, the weight relating to a likelihood that the packet is received from the one of the plurality of possible ports;

determining an expected port for the packet upon which the packet is expected to be received based on relative weights of the possible ports;

determining an actual port for the packet upon which the packet is actually received;

comparing the actual port to the expected port; and

providing spurious packet handling when the actual port does not correspond to the expected port.

2. Cancelled

3. (Original) The method of claim 1 wherein spurious packet handling includes discarding the packet.

4. (Original) The method of claim 1 wherein spurious packet handling includes generating an alert.

5. (Original) The method of claim 1 wherein the packet comprises an Internet Protocol packet.

6. (Currently amended) The method of claim 1 wherein ~~determining the expected port for the packet~~ calculating the plurality of possible ports further comprises:

determining a source network address for the packet; and

calculating ~~an~~ expected ~~path~~ paths for the packet according to routing trees of switches in the network, wherein ~~an ending~~ endings of the expected ~~path is~~ paths are the ~~expected port~~ possible ports.

7. (Currently amended) The method of claim 1 wherein determining an expected port for the packet further comprises:

generating a table, the table associating each one of a plurality of possible source network addresses with a ~~single port;~~ possible port and a weight

~~determining a source network address for the packet~~; and

applying the table to determine ~~single port associated with the source network address, the single port being~~ the expected port.

8. (Currently amended) A system for detecting spurious network traffic comprising:

receiving means for receiving a packet;

mapping means for calculating a plurality of possible ports from which the packet is expected to be received using a source network address of the packet, wherein each one of the plurality of possible ports has associated therewith a weight, the weight relating to a likelihood that the packet is received from the one of the plurality of possible ports;

first determining means for determining an expected port for the packet based on relative weights of the possible ports;

second determining means for determining an actual port for the packet;

comparing means for comparing the expected port and the actual port; and

handling means for providing spurious packet handling upon determining that the actual port does not correspond to the expected port.

9. Cancelled

10. (Currently amended) A switch for use in an internetwork, the switch comprising:

a plurality of ports, each port connected in a communicating relationship with at least one of a connected switch and a network;

a routing database, the routing database containing information relating to the internetwork; and

a processor, the processor configured to compare a first port of the plurality of ports through which a packet is received to a second port of the plurality of ports through which the packet is expected to be received, the processor further configured to provide spurious packet handling upon determining that the first port is different from the second port, and configured to generate an expected port table, the expected port table mapping each of a plurality of possible source network addresses to a plurality of possible ports of the switch, whereby a plurality of possible second ports are calculated by using a source network address of the packet, wherein each one of the plurality of possible second ports has associated therewith a weight, the weight relating to a likelihood that the packet is received from the one of the plurality of possible second ports.

11. (Original) The switch of claim 10 wherein the routing database includes a routing tree for each one of a plurality of connected switches.

12. (Original) The switch of claim 10 wherein the routing database includes a plurality of link state update packets and a plurality of routing update packets.

13. (Original) The switch of claim 10 wherein the second port is calculated by examining one or more routing trees stored in the routing database.

14. (Previously presented) The switch of claim 10 wherein the second port is calculated by examining a source network address of the packet.

15-17 Cancelled

18. (Original) The switch of claim 10 wherein the spurious network traffic handling includes discarding the packet.

19. (Original) The switch of claim 10 wherein the spurious network traffic handling includes generating an alert.

20. (Currently amended) An internetwork comprising a plurality of switches, each of the switches comprising:

a plurality of ports, each port connected in a communicating relationship with at least one of a connected switch and a network;

a routing database, the routing database containing information relating to the internetwork; and

a processor, the processor configured to compare a first port of the plurality of ports through which a packet is received to a second port of the plurality of ports through which the packet is expected to be received, the processor further configured to provide spurious packet handling upon determining that the first port is different from the second port, and configured to generate an expected port table, the expected port table mapping each of a plurality of possible source network addresses to a plurality of possible ports of the switch, whereby a plurality of possible second ports are calculated by using a source network address of the packet, wherein each one of the plurality of possible second ports has associated therewith a weight, the weight relating to a likelihood that the packet is received from the one of the plurality of possible second ports;

whereby spurious network traffic within the internetwork is detected.